

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1437446-0

Total Deleted Page(s) = 32

Page 24 ~ b5; b7E;
Page 25 ~ b5; b7E;
Page 26 ~ b5; b7E;
Page 27 ~ b5; b7E;
Page 28 ~ b5; b7E;
Page 29 ~ b5; b7E;
Page 30 ~ b5; b7E;
Page 31 ~ b5; b7E;
Page 32 ~ b5; b7E;
Page 33 ~ b5; b7E;
Page 34 ~ b5; b7E;
Page 35 ~ b5; b7E;
Page 36 ~ b5; b7E;
Page 37 ~ b5; b7E;
Page 38 ~ b5; b7E;
Page 39 ~ b5; b7E;
Page 40 ~ b5; b7E;
Page 41 ~ b5; b7E;
Page 42 ~ b5; b7E;
Page 43 ~ b5; b7E;
Page 44 ~ b5; b7E;
Page 45 ~ b5; b7E;
Page 49 ~ b5; b7E;
Page 50 ~ b5; b7E;
Page 51 ~ b5; b7E;
Page 52 ~ b5; b7E;
Page 53 ~ b5; b7E;
Page 54 ~ b5; b7E;
Page 55 ~ b5; b7E;
Page 56 ~ b5; b7E;
Page 57 ~ b5; b7E;
Page 60 ~ b5; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Spear-phishing SEC Scam**Date:** 03/13/2017**From:** NEW YORK

NY-C1

Contact: [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]b6
b7C
b7E**Case ID #:** 318D-NY-2142524-FF (U) Spear-phishing SEC Scam**Synopsis:** (U) To open an Asset Forfeiture subfile.**Details:**

An article on the FORTUNE website reported a cyber spear-fishing scam in which emails, purportedly from the Securities and Exchange Commission, were sent to companies in an effort to obtain inside information. The messages specifically targeted individuals in positions responsible for SEC filings. When individuals clicked on instructions within a MICROSOFT Word file in the emails, the attackers were granted access to internal networks. FORTUNE reported that the spear-phishing attack was discovered in February by a company called FIREEYE, which was able to intercept some of the emails. FIREEYE believed the attackers to be an Eastern European crime syndicate attempting to achieve financial gain by trading based on inside information.

This subfile will serve as a repository for forfeiture-related materials.

◆◆

UNCLASSIFIED

UNCLASSIFIED

Title: (U) 2017 03 08 Opening
Re: 318D-NY-2142524, 03/08/2017

On March 08, 2017, [REDACTED] of the US Attorney's Office for the Eastern District of New York (EDNY) concurred with the opening of the captioned investigation. On March 08, 2017, Supervisory Special Agent [REDACTED] of the Complex Financial Crimes Unit concurred with the opening of the captioned investigation.

b6
b7C

Initial investigative steps will include identifying witnesses and potential victims; coordinating with the SEC; obtaining and reviewing suspect emails; reviewing publicly available information.

The captioned investigation will be opened and assigned to Special Agent (SA) [REDACTED] FBI New York Squad C-1.

b6
b7C

◆◆

UNCLASSIFIED

≡ FORTUNE | Tech

🔍 SEARCHSUBSCRIBE

Most Powerful Women
Trump to Meet With Laurene Powell Jobs, Widow of Apple Co-Founder Steve Jobs



4:02

Wall Street
Wall Street Spent \$2 Billion Trying to Influence the 2016 Election



1:51

Market Intelligence
Here's Why Snap Shares Are Looking Up Again



4:02

World's Most Admired Companies
Amazon Is About to Open Bookstore Number 10



4:02



Andrew Harrer/Bloomberg via Getty Images

PointCloud

Fake SEC Emails Target Execs for Inside information

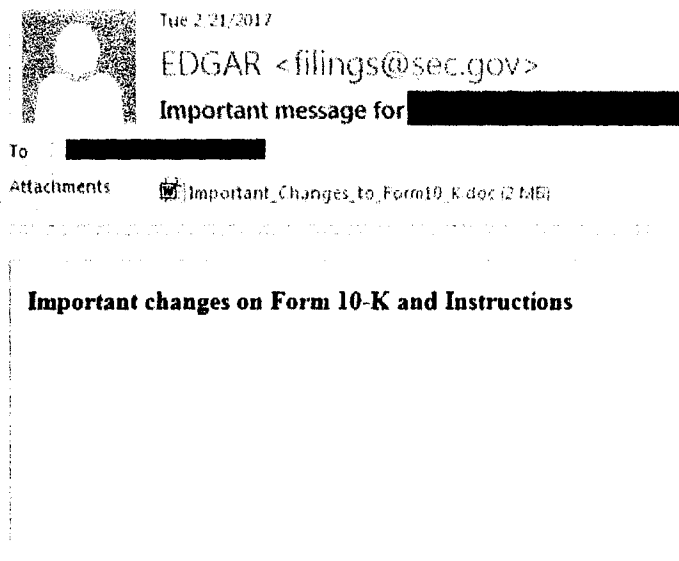
Jeff John Roberts
Mar 07, 2017



Cyber scammers are using a new trick to get confidential corporate information: They are sending spoofed emails, purporting to be from the Security and Exchange Commission, and aiming them at lawyers, compliance managers, and other company officials who file documents with the SEC.

The security company FireEye (FEYE, +0.52%) discovered the ruse in late February, when it intercepted suspicious emails targeted at companies in sectors ranging from transportation to banking to retail. FireEye, which set out its findings in a blog post, believes the scammers are likely to be an Eastern European criminal syndicate looking to make money by trading on inside information.

In some cases, FireEye says corporate executives did click on a fake Microsoft Word file included with the email. Here's a screenshot of the email, which contains little text and appears to come from EDGAR, which is the base of the SEC's filing service:



Those who clicked on instructions in the Word document granted the attackers access to internal corporate networks, though FireEye says, in the case of its customers, it was able to contain and evict the scammers within hours. (In many cases, the company says it was able to intercept them altogether).

The reach of the scam, however, could be much broader than the activity detected by FireEye.

The email attacks in question, known as "spear-phishing" are effective because they are addressed to specific people and appear to be from a legitimate source. In the case of the fake SEC emails, the targets included corporate officials with titles like SEC Reporting Manager and Senior Legal Specialist—the very people, in other words, responsible for securities filings, and who could expect to receive an email from the SEC.

Get Data Sheet, Fortune's technology newsletter.

John Miller, a director of threat intelligence at FireEye, described the attackers as among "the most sophisticated financial actors" and said their methods were similar to hackers who targeted ATM machines and other parts of the banking system. He also warned the hacking tools they sought to install were particularly insidious.

"It's the Swiss army knife of malware. It lets you do whatever you want to with the compromised system," Miller said.

In response to whether it was familiar with the recent cyber-phishing campaign, a spokesperson for the SEC declined comment.

SPONSORED STORIES

Recommended by



How To Watch 600+ Hours of
Quality, Ad-Free Documentaries
Los Angeles Times



China is developing a hypersonic
space plane that makes the
Space Shuttle look primitive
Digital Trends

Related Content

PointCloud
John Deere Floats Drones as the Next Big Tool
for Construction Workers



FOR

PointCloud
Here's Why HPE Just Paid \$1 Billion for
Nimble Storage



FOR

PointCloud



Pivotal Claims Big Growth for Its Cloud


FORTUNE | Tech

SEARCH SUBSCRIBE

SPONSORED STORIES



Gigi Hadid's Go-To Shoe Is Surprisingly Affordable
WhoWhatWear



5 Shirt Mistakes You Need To Stop Making
Proper Cloth



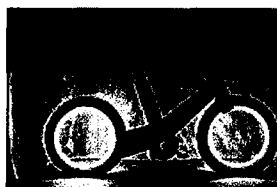
The F-15 Is No Match For This Plane
theBrofessional.net



We Can Guess Your Education Level With This Simple Quiz
Definition



Librarians Love It - The One Website Book Lovers Need to Know
The Book Insider



The hubless, carbon-fiber Cyclotron bike looks straight out of 'Tron'
Digital Trends



Top 5 Ancestry Tests that Will Teach You About Your Family's History
www.top10bestdnatesting.com



Retail Shoppers Are Moving to Virtual Reality [White Paper]
Cognizant

Next Up

Tech

Trump to Meet With Laurene Powell Jobs, Widow of Apple Co-Founder Steve Jobs

Laurene Powell Jobs, a prominent Silicon Valley philanthropist and widow of Apple AAPL co-founder Steve Jobs, was scheduled to meet with President Donald Trump on Wednesday. Powell Jobs, who was

FORTUNE

≡ FORTUNE | Tech

🔍 SEARCHSUBSCRIBE

Next Up

Tech

Trump to Meet With Laurene Powell Jobs, Widow of Apple

Co-Founder Steve Jobs

Laurene Powell Jobs, a prominent Silicon Valley philanthropist and widow of Apple AAPL co-founder Steve Jobs, was scheduled to meet with President Donald Trump on Wednesday. Powell Jobs, who was

FORTUNE

More Coverage



Cybersecurity

U.S. Intel and Law Enforcement Agencies Were Aware of CIA Breach Since Last Year

U.S. intelligence and law enforcement officials said on Wednesday that they have been aware since the end of last year of a security breach at the CIA that led to anti-secrecy group WikiLeaks

FORTUNE



Market Intelligence

Here's Why Snap Shares Are Looking Up Again

Shares of Snap Inc rebounded on Wednesday following a steep selloff while an initial rush to short sell the stock appeared to be slowing. The owner of the Snapchat messaging app had fallen sharply

FORTUNE

SEARCH SUBSCRIBE



World's Most Admired Companies

Amazon Is About to Open Bookstore Number 10

It was a big deal when Amazon opened a physical bookstore in 2015, symbolizing how the company's retail ambitions extend beyond its online operations. Today, the move looks much more than

FORTUNE**More Coverage**

Cybersecurity

U.S. Intel and Law Enforcement Agencies Were Aware of**CIA Breach Since Last Year**

U.S. intelligence and law enforcement officials said on Wednesday that they have been aware since the end of last year of a security breach at the CIA that led to anti-secrecy group WikiLeaks

FORTUNE

 **FORTUNE** | Tech SEARCH  SUBSCRIBE

Market Intelligence

Here's Why Snap Shares Are Looking Up Again

Shares of Snap Inc rebounded on Wednesday following a steep selloff while an initial rush to short sell the stock appeared to be slowing. The owner of the Snapchat messaging app had fallen sharply

FORTUNE

World's Most Admired Companies

Amazon Is About to Open Bookstore Number 10

It was a big deal when Amazon opened a physical bookstore in 2015, symbolizing how the company's retail ambitions extend beyond its online operations. Today, the move looks much more than

FORTUNE**Most Popular Stories**

1

Here's What Hillary Clinton Wants You to Remember This International Women's Day

Here's What Hillary Clinton Wants You to Remember This International Women's Day

2

These 3 Powerful Groups Are Slamming the GOP's Obamacare Replacement Plan

These 3 Powerful Groups Are Slamming the GOP's Obamacare Replacement Plan

3

You're Not Cool Enough To Get the Secret Version of Tinder

4

You're Not Cool Enough To Get the Secret Version of Tinder

4

Starbucks Is Now Offering Whiskey Barrel-Aged Coffee

5

Starbucks Is Now Offering Whiskey Barrel-Aged Coffee

5

There's Now a Statue of a Fearless Little Girl Staring Down Wall Street's Charging Bull

There's Now a Statue of a Fearless Little Girl Staring Down Wall Street's Charging Bull

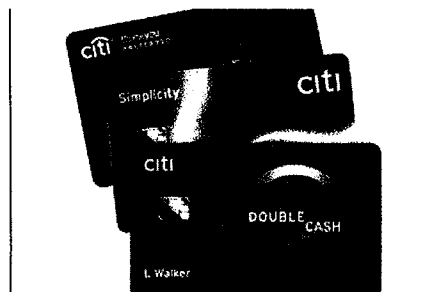
Sponsored Financial Content

dianomi



50 Billion of These Will Be In Use by 2020

Banyan Hill



Before Applying For A Credit Card, Check If You Pre-Qualify

Citi

≡ **FORTUNE** | Tech

J.P.Morgan
Asset Management

🔍 SEARCHSUBSCRIBE

3 Ways to Help Improve Retirement Outcomes
J.P. Morgan Funds



Hedging inflation w/real estate: How we judge quality & why it matters
FlexShares ETFs

More from FORTUNE.com

Finance

Wall Street Spent \$2 Billion Trying to Influence the 2016 Election

Wall Street has really thrown its money around Washington the past couple of years. Banks, trade associations, and other related financial interests spent \$2 billion on trying to influence

FORTUNE

Finance

PIMCO Just Replaced the Managers of Bill Gross' Former Bond Fund SEARCH  SUBSCRIBE

Pacific Investment Management Co (Pimco) is replacing the full slate of managers on its Total Return Active Exchange-Traded Fund and changing its name, a spokeswoman for the fund management company

FORTUNE

MPW

Here's Why the Defiant Girl Statue in Front of the Wall Street Bull Is So Important

Between 4 a.m. and 6 a.m. on Tuesday, lower Manhattan got its newest resident: a 50-inch defiant little girl, cast in bronze, standing opposite Wall Street's famous charging bull. State

FORTUNE

Finance

Snap CEO Evan Spiegel Will Get \$822 Million for Taking the Company Public

Snapchat's then-private owners really wanted CEO Evan Spiegel to take their photo-based social media company public. In mid-2015, Snap's board of director's agreed to award

FORTUNE

≡ FORTUNE | Tech

🔍 SEARCH SUBSCRIBE



MPW

Watch Live: House Dems Hold Event Honoring International Women's Day

Democrats including House Minority Leader Nancy Pelosi and the Democratic Women's Working Group will hold a press event for International Women's Day on the steps of the U.S. Capitol

FORTUNE

Leadership

American Healthcare Act Woes Will Hamper the Rest of Trump's Agenda

The Obamacare replacement plan premiered by House Republican leaders Tuesday met with an ugly, bruising reception. Ultraconservative House members tore into the proposal as a warmed-over version of

FORTUNE



Tech

The WikiLeaks CIA Reveal Has Some Tech Firms Scrambling for Fixes

Tech companies must rapidly step up information sharing to protect users from prying eyes, a security software executive said on Wednesday after WikiLeaks released a trove of documents

FORTUNE

≡ FORTUNE | Tech

🔍 SEARCHSUBSCRIBE

Leadership

China Gives Preliminary Approval For 38 New Trump Trademarks

China has given preliminary approval for 38 new Trump trademarks, opening opportunities for the president and his family to develop branded businesses in the country, including hotels, golf

FORTUNE



MPW

House Democratic Women Are Staging a Walkout for 'Day Without a Woman'

Democratic congresswomen are staging a walkout Wednesday in support of "A Day Without a Woman." Rep. Lois Frankel (D-Fla.), the chairwoman of the Democratic Women's Working Group,

FORTUNE



 **FORTUNE** | Tech SEARCH  SUBSCRIBE

Photography

Celebrating Fortune's First Photographer: Margaret Bourke-White

The history of this over 85-year-old magazine has been documented extensively. Fortune came at a time when the press largely ignored business and when the U.S. was in the beginning of the

FORTUNE

[Customer Service](#) [Site Map](#) [Privacy Policy](#) [Advertising](#) [Ad Choices](#) [Terms of Use](#) [Your California Privacy Rights](#) [Careers](#)

FORTUNE © 2017 Time Inc. All rights reserved.

All products and services featured are based solely on editorial selection. FORTUNE may receive compensation for some links to products and services on this website.

Quotes delayed at least 15 minutes. Market data provided by Interactive Data. ETF and Mutual Fund data provided by Morningstar, Inc. Dow Jones Terms & Conditions: <http://www.djindexes.com/mdsidx/html/tandc/indexestandcs.html>. S&P Index data is the property of Chicago Mercantile Exchange Inc. and its licensors. All rights reserved. Terms & Conditions. Powered and implemented by Interactive Data Managed Solutions

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Access Request Letter**Date:** 03/13/2017**From:** NEW YORK

NY-C1

Contact: [REDACTED]**Approved By:** SSA [REDACTED]b6
b7C
b7E**Drafted By:** [REDACTED]**Case ID #:** 318D-NY-2142524 (U) Spear-phishing SEC Scam**Synopsis:** (U) To document an SEC access request.**Full Investigation Initiated:** 03/08/2017**Enclosure(s):** Enclosed are the following items:

1. (U) SEC Access Request Letter
2. (U) SEC Access Granted Letter

Details:

On March 09, 2017, the writer emailed an "access request" letter to [REDACTED] at the SECURITIES AND EXCHANGE COMMISSION (SEC). The letter, which was addressed to Associate Regional Director [REDACTED] [REDACTED] served to request access to the investigative and other non-public files of the SEC.

b6
b7C

On March 10, 2017, the writer received an email from [REDACTED] at the SEC, which contained a letter from [REDACTED] granting the requested access. The letter identified [REDACTED] as the initial SEC point of contact.

b6
b7C

◆◆

UNCLASSIFIED



U.S. Department of Justice

Federal Bureau of Investigation

26 Federal Plaza
New York, NY 10278

March 9, 2017

Mr. [REDACTED]
Associate Regional Director
U.S. Securities and Exchange Commission
New York Regional Office
3 World Financial Center
Suite 400
New York, NY 10281

b6
b7C

Re: Case NY-09645

Dear Mr. [REDACTED]

We request access to the investigative and other non-public files of the U.S. Securities and Exchange Commission ("Commission") related to the above-captioned matter. This request is made in connection with an ongoing lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, a criminal or civil statute or regulation, rule or order issued pursuant thereto, being conducted by The Federal Bureau of Investigation.

We understand that the files in this matter contain "financial records" of "customers," as those terms are defined in the Right to Financial Privacy Act of 1978 [12 U.S.C. §§3401-22]. We have reason to believe that that information is relevant to our investigation.

We will establish and maintain such safeguards as are necessary and appropriate to protect the confidentiality of files to which access is granted and information derived therefrom. The files and information may, however, be used for the purpose of our investigation and/or proceeding and any resulting proceedings. They also may be transferred to criminal law enforcement authorities and self-regulatory organizations subject to our oversight. We shall notify you of any such transfer and use our best efforts to obtain appropriate assurances of confidentiality.

Other than as set forth in the preceding paragraph, we will:

- make no public use of these files or information without prior approval of your staff;

- notify you of any legally enforceable demand for the files or information prior to complying with the demand, and assert such legal exemptions or privileges on your behalf as you may request; and
- not grant any other demand or request for the files or information without prior notice to and lack of objection by your staff.

We recognize that until this matter has been closed, the Commission continues to have an interest and will take further investigatory or other steps as it considers necessary in the discharge of its duties and responsibilities.

Should you have any questions, please contact:

Special Agent [REDACTED]
Federal Bureau of Investigation
New York Field Office
26 Federal Plaza
New York, New York 10278

[REDACTED]

b6
b7C
b7E

Sincerely,

Michael C. McGarrity
Special Agent in Charge
Federal Bureau of Investigation

By

[REDACTED]

[REDACTED]

Acting Supervisory Special Agent
Federal Bureau of Investigation

b6
b7C

[redacted] (NY) (FBI)

From: [redacted]
Sent: Friday, March 10, 2017 11:52 AM
To: [redacted] (NY) (FBI)
Cc:
Subject: Access Request NY-09645
Attachments: Access Request 2017-6473 (MNY-09645).pdf

b6
b7C

Please see attached.

From: [redacted]
Sent: Friday, March 10, 2017 11:10 AM
To: [redacted]
Subject:

b6
b7C

Hi [redacted]
Can you please process for [redacted]?
Thanks!



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
NEW YORK REGIONAL OFFICE
BROOKFIELD PLACE, 200 VESEY STREET,
SUITE 400
NEW YORK, NY 10281-1022

WRITER'S DIRECT DIAL LINE

TELEPHONE: (212) 336-0181
FACSIMILE: (212) 336-1323

March 10, 2017

Michael C. McGarrity
Special Agent in Charge
Federal Bureau of Investigation
New York Field Office
26 Federal Plaza
New York, NY 10278

Re: Certain Spoofed Emails (MNY-09645)

Dear Mr. McGarrity:

Your request, by letter dated March 9, 2017, for access to Commission files has been granted. In granting access, the Commission has relied upon your assurances that, except as set forth in your letter, your office will:

Provide such safeguards as are necessary and appropriate to protect the confidentiality of these files;

Make no public use of these files or information without prior approval of our staff;

Notify us of any legally enforceable demand for the files or information prior to complying with the demand, and assert such legal exemptions or privileges on our behalf as we may request; and

Not grant any other demand or request for the files or information without prior notice or over our objection.

The files in this matter may contain "financial records" of "customers" of "financial institutions," as those terms are defined in the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401-22]. In the event that another federal agency should seek information from those files from your agency, we urge you to have the federal agency contact us before you provide such information.

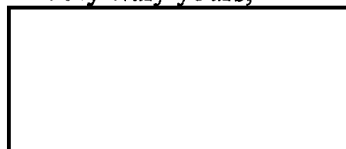
Michael C. McGarrity
March 10, 2017
Page 2

The Commission makes no recommendation with respect to the investigation or prosecution by your office. In addition, until this matter is closed, the Commission continues to have an interest and will take such further investigatory or other steps as it considers necessary in the discharge of its duties and responsibilities.

The files to which access has been granted are being retained by the New York Regional Office of the Commission. Your representative should contact [redacted] at [redacted] to make arrangements to review the files. I would also appreciate it if you would inform that person in the event that your agency institutes public proceedings based upon information that you obtain as a result of this grant of access.

b6
b7C

Very truly yours,

A rectangular box with a black border, used to redact the signature of the Senior Associate Regional Director.

Senior Associate Regional Director

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) FIREEYE Report**Date:** 03/17/2017**From:** NEW YORK

NY-C1

Contact: [REDACTED]**Approved By:** SSA [REDACTED]b6
b7C
b7E**Drafted By:** [REDACTED]**Case ID #:** 318D-NY-2142524 (U) Spear-phishing SEC Scam**Synopsis:** (U) To document a report obtained from FIREEYE regarding their investigation into the SEC spear-phishing scam.**Full Investigation Initiated:** 03/08/2017**Enclosure(s):** Enclosed are the following items:

1. (U) FIREEYE SEC Spear-phishing Report
2. (U) FIREEYE Indicators

Details:

On March 15, 2017, with the assistance of FIREEYE contacts [REDACTED]

[REDACTED] and [REDACTED]
(support@fireeye.com, [REDACTED] the writer obtained the FIREEYE
threat intelligence report associated with the FORTUNE article [REDACTED]
[REDACTED]

b6
b7C
b7E

The report, which was dated March 01, 2017, contained information presented in the FORTUNE article and indicated that FIREEYE had high confidence that an entity called FIN7 was connected to the attack. The report also stated that FIREEYE had identified 11 targeted organizations within the United States and, more specifically, within the financial services, transportation, retail, education, IT services, and electronics sectors.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) FIREEYE Report
Re: 318D-NY-2142524, 03/17/2017

FIREEYE'S report noted that many of the targeted organizations also had an international presence. While the report did not definitively identify the goal of the attackers, it did speculate that those involved might be pursuing securities fraud, investment abuse, or other fraud types.

The FIREEYE report was attached as a 1A package.

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) FIREEYE Conference Call**Date:** 04/04/2017**From:** NEW YORK

NY-C1

Contact: [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]b6
b7C
b7E**Case ID #:** 318D-NY-2142524 (U) Spear-phishing SEC Scam**Synopsis:** (U) To document a conference call with FIREEYE personnel.**Full Investigation Initiated:** 03/08/2017**Enclosure(s):** Enclosed are the following items:

1. (U) FIREEYE Call Notes

Details:

On March 23, 2017 at 2:00 p.m., Special Agents [REDACTED] and [REDACTED] participated in a conference call with representatives from FIREEYE [REDACTED] [REDACTED] hereinafter referred to as "FIREEYE". Also present for the conversation were [REDACTED] and [REDACTED] from the United States Attorney's Office for the Eastern District of New York, and [REDACTED] from the Securities and Exchange Commission (SEC). FIREEYE provided the following information:

b6
b7C

Eleven companies were targeted in the scam. The eleven companies were all targeted in 2017. Two or three individuals at the companies clicked the link in the MICROSOFT Word document. Nothing suggested the intruders successfully accessed inside information. The intrusion was caught early in its life-cycle.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) FIREEYE Conference Call
Re: 318D-NY-2142524, 04/04/2017

The spear-phishing emails were sent from a compromised GODADDY account. FIREEYE believed the attack was linked to Eastern European cyber-criminals, specifically FIN7. The spear-phishing attack utilized CARBANAK malware. CARBANAK was previously used by Eastern European groups. Historically, CARBANAK was called ARBANAK by Eastern European companies. The oldest attacks associated with CARBANAK traced back to 2013. These attacks involved activity in areas such as Russia. The malware was shared, and had an underground distribution. There was a nexus between Eastern European criminal groups and CARBANAK.

The spear-phishing emails sent to the targeted companies were addressed to specific personnel. The targeted individuals were publicly associated with SEC filings. The spoof emails were made to look like they were from EDGAR. The emails were spoofed to appear to be sent from the email address "filings@sec.gov". In a couple of customer cases, the intruders pulled down back doors. The intruders also pulled down CARBANAK and another tool. DNS malware was used during the attacks.

FIREEYE found older attacks they believed were linked to the 2017 attacks. One similar attack was in the summer of 2015, and two similar attacks were in the summer of 2016. These attacks also involved DNS malware and were related to SEC filings.

b5
b7E

UNCLASSIFIED

UNCLASSIFIED

Title: (U) FIREEYE Conference Call

Re: 318D-NY-2142524, 04/04/2017

FIREEYE was unable to provide a list of the targeted companies due to their policies and agreements. FIREEYE agreed to contact representatives at the companies to provide FBI contact information.

◆◆

UNCLASSIFIED

8/3/23/17

* POL

- SEC

b6
b7C

- w/ company for a year;

b6
b7C

- SEC - possibly same actor - same DNS Text malware - summer 2015 + summer 2016. updated report will link old + new attacks

- cannot provide additional details regarding companies that were victims

b5
b7E

1 of 2

- At companies - emails - addressed to specific name or personnel - names publicly associated w/ SEC filings

- Spoof email - looks like Edgar (older email's the same vein; filings @ sec.gov;

- in a couple customer cases, pulled down backdoors; pulled down Carbanet & another tool

- Timeline: blogged about occurred in 17 } used DMS malware
2-16
1-15

- How Eastern Euro?

- loose association based on Carbanet

- historically, Carbanet called Abnaki by Eastern companies

- oldest attacker go to 2013 area

- malware seems to be shared, has underground distribution

- seems to be Nexus of East. Euro groups using Carbanet

Fin 7 - Retail/hospitality industries

- 28 April 18 email

- 2 or 3 clicked link / Bell victim

- 2017 - 11 companies targeted

- emails sent from compromised Godaddy account

- caught early on in lifecycle of intrusion

- nothing specific regarding information that might be compromised

2 of 2

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Closing Communication**Date:** 05/17/2017**From:** NEW YORK

NY-C1

Contact: [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]b6
b7C
b7E**Case ID #:** 318D-NY-2142524 (U) Spear-phishing SEC Scam**Synopsis:** (U) To document closing of captioned investigation**Full Investigation Initiated:** 03/08/2017**Details:**

Captioned investigation was opened on March 8, 2017 based on reports from Fireeye which claimed certain of their clients, which were publicly traded companies, were targeted in a phishing scam. The specific targets within the companies were individuals with responsibility over financial reporting, and the phishing emails claimed to be from an official Securities and Exchange Commission (SEC) account. The SEC opened their own civil investigation, and the United States Attorney's Office for the Eastern District of New York (EDNY) concurred with the opening of a parallel criminal investigation. Investigation was to focus on trading patterns in the stock of the victim companies, to determine if the information was used for profitable trading.

Due to confidentiality agreements, Fireeye could not release the names of their clients who were targeted. Fireeye reached out to the customers and advised the FBI had an open investigation, and instructed clients to contact writer should they be willing to cooperate with the investigation. One client, [REDACTED] contacted writer, and advised they were targeted but stopped the intrusion

b7E

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Closing Communication
Re: 318D-NY-2142524, 05/17/2017

before any information was taken. After several additional attempts to reach out to clients, no other companies have come forward as willing to cooperate in the investigation.

Since there are no identified victims, and only one potential victim identified, there are no trading records to review. Similarly, with no victims coming forward, there are no additional emails to review. The identity of the group responsible for the hack is unknown, but believed to be a group previously identified as FIN7. FIN7 is believed to be an Eastern European criminal enterprise, but their location is unknown.

Since there are no investigative leads to follow, and no identified victims, EDNY declined prosecution of the case. Should any victims decide to contact the FBI, the investigation could be re-opened.

All logical and reasonable investigative steps were taken. Sufficient personnel and financial resources were expended. All investigative steps and methods have been completed. There were no leads set, and no evidence collected.

Writer requests captioned investigation be closed due to prosecutorial declination.

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) 2017 03 08 Opening**Date:** 03/08/2017**CC:** [REDACTED]**From:** NEW YORK

NY-C1

Contact: [REDACTED]b6
b7C
b7E**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 318D-NY-2142524 (U) Spear-phishing SEC Scam**Synopsis:** (U) To open a new full investigation related to a spear-fishing SEC scam.**Full Investigation Initiated:** 03/08/2017**Enclosure(s):** Enclosed are the following items:

1. (U) FORTUNE Article

Details:

An article on the FORTUNE website reported a cyber spear-fishing scam in which emails, purportedly from the Securities and Exchange Commission, were sent to companies in an effort to obtain inside information. The messages specifically targeted individuals in positions responsible for SEC filings. When individuals clicked on instructions within a MICROSOFT Word file in the emails, the attackers were granted access to internal networks. FORTUNE reported that the spear-phishing attack was discovered in February by a company called FIREEYE, which was able to intercept some of the emails. FIREEYE believed the attackers to be an Eastern European crime syndicate attempting to achieve financial gain by trading based on inside information.

UNCLASSIFIED